

1 / 2

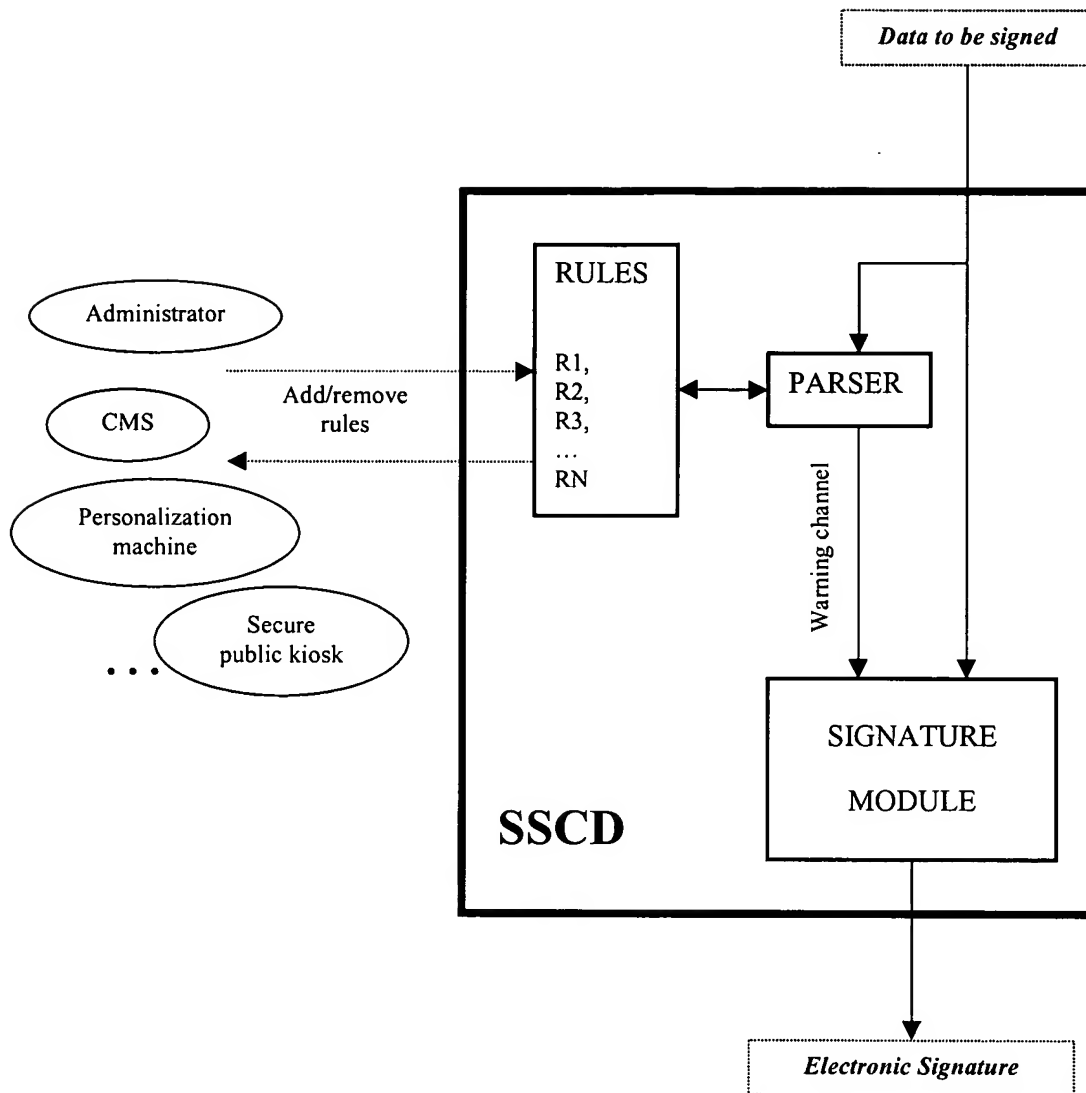


Fig. 1

Fund Transfers for Lukasz Wlodarczyk

account to debit	24368 188234 00300
account to credit	28547 487162 00300
Amount	1400
Currency	<input checked="" type="radio"/> US Dollars <input type="radio"/> Euros

Sign transaction
Cancel transaction

Fig. 2

DATA TO BE SIGNED

| hashing module (called repeatedly until all input data is processed)
 | [uses algorithms such as SHA-1 or MD5]

√

hash of the data to be signed

| padding module (PKCS#1 format for example)

√

padded hash of the data to be signed

| private key operation engine (asymmetric crypto)
 | [uses algorithms such as RSA, DSA or EC]

√

SIGNATURE (signed padded hash)

Fig. 3